SIMMONS HANLY CONROY, LLC
Jason 'Jay' Barnes (admitted *pro hac vice*)
An Truong (admitted *pro hac vice*)
Eric Johnson (admitted *pro hac vice*)
112 Madison Avenue, 7th Floor
New York, NY 10016
Telephone: (212) 784-6400
Facsimile: (212) 213-5949
jaybarnes@simmonsfirm.com
atruong@simmonsfirm.com
ejohnson@simmonsfirm.com

KIESEL LAW LLP
Jeffrey A. Koncius, State Bar No. 189803
Nicole Ramirez, State Bar No. 279017
Mahnam Ghorbani, State Bar No. 345360
8648 Wilshire Boulevard
Beverly Hills, CA 90211-2910
Telephone: (310) 854-4444
Facsimile: (310) 854-0812
koncius@kiesel.law
ramirez@kiesel.law
ghorbani@kiesel.law

SCOTT+SCOTT ATTORNEYS AT LAW LLP
Joseph P. Guglielmo (admitted *pro hac vice*)
The Helmsley Building
230 Park Ave, 17th Floor
New York, NY 10169
Telephone: (212) 223-6444
Facsimile: (212) 223-6334
jguglielmo@scott-scott.com

LOWEY DANNENBERG, P.C.
Christian Levis (admitted *pro hac vice*)
Amanda Fiorilla (admitted *pro hac vice*)
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Facsimile: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
Michael W. Sobol, State Bar. No. 194857
Melissa Gardner, State Bar No. 289096
Jallé H. Dafa, State Bar No. 290637
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: (415) 956-1000
Facsimile: (415) 956-1008
msobol@lchb.com
mgardner@lchb.com

Attorneys for Plaintiffs and the Proposed Class
Additional Counsel Listed on Signature Page

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

JOHN DOE, *et al.*, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

This document applies to: All Actions

Case No.: 3:23-cv-02431-VC
Consolidated with: 3:23-cv-02343-VC

PLAINTIFFS' REPLY IN SUPPORT OF THE MOTION FOR PRELIMINARY INJUNCTION & RESPONSE IN OPPOSITION TO GOOGLE'S MOTION TO DISMISS

Judge: Hon. Vince Chhabria
Date: September 21, 2023
Time: 10:00 AM
Ctrm: 4, 17th Floor

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF AUTHORITIES

Page

Cases

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

Regulations

I. INTRODUCTION

Google's combined opposition to Plaintiffs' motion for preliminary injunction and motion to dismiss under Rule 12(b)(6) (Dkt. 48, "MTD" or "Motion") does not address the core issues before the Court: whether Google collected patients' Health Information through Google Source Code embedded in Health Care Providers' web properties in violation of state and federal law, and whether Google should be permitted to continue doing so until a final judgment in this action. Rather, Google ignores much of the evidence submitted by Plaintiffs' experts, mischaracterizes the law, and tries to restrict the conduct at issue solely to Google Analytics. But Plaintiffs' allegations and evidence show that Google's misconduct far exceeds Google Analytics, and includes Google Ads, Google Display Ads, Google Tag, Google Tag Manager, Google Firebase SDK, Google APIs, and YouTube, as well as offline "matching" of sensitive data. Moreover, Plaintiffs' experts present evidence that Google's Source Code does in fact track and redirect patient identifiers and Health Information, including communications in and outside of "secure" patient portals in real time. These core facts are unrebutted. They demonstrate the merits of Plaintiffs' claims and support granting the injunctive relief requested.

Google's other arguments are equally unavailing. *First*, Google cannot avoid liability by shifting the blame to Health Care Providers. At best, Google shows that *both* Google and Health Care Providers engage in wrongful conduct. *Second*, Google's argument that Plaintiffs and class members consented to Google intercepting their Health Information is belied by its express promise not to do so. Purported browser-wrap "disclosures" (if any) from Health Care Providers are irrelevant and cannot override Google's clear and explicit statements. *Third*, Google's attempt to downplay its interception of Health Information by claiming Plaintiffs' allegations are "conclusory" and involve "pseudonymous" data is inconsistent with law and the facts alleged. Plaintiffs allege Google intercepted identifiable Health Information relating to their actual appointments and medical conditions, which numerous courts in this District recognize is protected by federal and state law. *Fourth*, Google claims to protect against the use of Health Information for personalized advertising. But advertising use, let alone personalized advertising, is not required for any of Plaintiffs' claims, which arise from the improper *interception* of Health Information. As

demonstrated below, Google does not have any actual safeguards that prevent the interception of Health Information in the first instance aside from wholly ineffective (and unenforced) policies.

In sum, Google's brief is littered with mischaracterizations and mis-directions that fail to rebut key allegations and evidence, and its varied arguments are ill supported. Plaintiffs' Motion for Preliminary Injunction should be granted and the MTD denied.

II. STATEMENT OF ISSUES TO BE DECIDED

With respect to the motion for preliminary injunction, the issues are those set forth in Plaintiffs' moving brief (*see* Dkt. 42, "MPI", at 1). With respect to the motion to dismiss, the issue is whether Plaintiffs have adequately pled their claims.

III. STATEMENT OF RELEVANT FACTS

A. GOOGLE'S UNLAWFUL ACQUISITION OF HEALTH INFORMATION

Plaintiffs allege that Google intercepts Health Information—including communications with Health Care Providers and patient identifiers—without patient consent. *See* CCAC ¶¶ 4-7, 19-31, 39-42, 333, 385, 396-403. Google does so through Google Source Code, which causes Google tracking cookies to be lodged on patients' browsers, and surreptitiously instructs the tracking, re-direction and collection of Health Information. *Id.* ¶¶ 41, 48, 53, 55, 57, 59-62, 64, 77-83, 88-94, 96-101. Plaintiffs' experts confirm these allegations. *See infra* § III.A.3.

1. The Google Products At-Issue

Google wrongly attempts to cabin Plaintiffs' claims to only one of Google's tracking technologies (Google Analytics ("GA")), but the case is not so limited. Plaintiffs' allegations include Google Ads, Google Display Ads, Google Tag, Google Tag Manager, Google Firebase SDK, Google APIs, and YouTube (CCAC ¶ 6), as well as offline acquisition (*id.* ¶¶ 102-10). Plaintiffs have alleged that Google Source Code for *all* of these products (not just GA): *individually* tracks and re-directs patients' Health Information to Google (*id.* ¶¶ 39-101, 102-10); *collectively* work together to form a virtually inescapable network of data tracking and collection by Google across the Health Care Provider web properties (*id.* ¶¶ 144-67); and, after collection, Google is able to associate, aggregate, and link Health Information to individual patient identifiers for advertising and other purposes across these various systems (*id.* ¶¶ 111-42, ¶¶ 161-77).

2. The Health Information At-Issue

Plaintiffs allege Google collects and intercepts Plaintiffs' and class members' unique identifiers and the content of their communications with their Health Care Providers, *e.g.,* detailed URLs, patient registrations, patient access to and communications within purportedly "secure" patient portals, and communications relating to specific doctors, appointment requests, symptoms, conditions, treatments, insurance, and prescription drugs. *See* CCAC ¶¶ 2, 19-31, 33-36. The CCAC further details, based on expert analysis, the specific transmissions made to the Google products at-issue. *See id.* ¶¶ 52-65 (GA), ¶¶ 77-83 (Google Ads), ¶¶ 89-94 (Google Display Ads), ¶¶ 96-101 (Tag, Tag Manager, Firebase SDK, APIs, and YouTube).

3. Plaintiffs' Experts Confirm the Allegations of Unauthorized Tracking and Collection of Health Information via the Google Source Code

Plaintiffs' experts confirm the allegations in the CCAC. Software analyst Richard M. Smith confirms the presence of Google Source Code on eleven sample Health Care Provider web-properties and describes the identifiers, content, and Health Information that Google tracks, intercepts and receives, via Google Source Code. *See* Dkt. 42-1, Smith Decl., ¶¶ 17 *et seq.*[1] This includes the transmission of unique identifiers (*e.g.,* cookie identifiers), URLs, IP addresses, User-Agents, communications content from authenticated (*e.g.,* patient portals) and unauthenticated web pages. *See id.* ¶¶ 61 *et seq*. These data parameters are consistent with the Health Information alleged by Plaintiffs. *See* CCAC ¶¶ 33-101. Smith further confirms that the transmissions to Google occur simultaneously with patients' communications to their Health Care Providers. *See, e.g.,* Smith Decl. ¶ 36. In addition, Smith shows that Google Source Code allows Google to collect and match cookies from other sites using GA. *See id.* at ¶¶ 100-05.

Similarly, data analyst Dr. Timothy Libert confirms that of approximately 6,046 web

[1] Contrary to Google's assertion that the Smith Declaration only shows "some websites use GA," (MTD at 11), Smith confirmed that *all eleven* of the web properties analyzed contained Google Source Code that transmitted Health Information to the Google products at issue. Any argument that *every* Health Care Provider property in the U.S. must be analyzed lacks legal support. The fact of occurrence is undisputed and the evidence supports classwide application. In fact, in other litigation, Google acknowledged that its source code is designed to work identically across web pages. *See* Barnes Suppl. Decl. ¶¶ 12-21. Plaintiffs need not test every web property on the Internet, let alone do so to prove what is not in dispute. On July 19, 2023, Plaintiffs provided Google with the list of Health Care Provider web properties where Google Source Code appears. *Id*. ¶¶ 5-6. To date, Google has not disputed evidence of this broad range of Google's health tracking. *Id.*

properties, Google Source Code was detected on 87%; with Google Analytics present on 67%, Google Ads 58%, Google Display Ads 59%, Google Tag Manager 69%, Google APIs 66%, and YouTube 19%. *See* Dkt. 44, Libert Decl. ¶¶ 9, 23.

Further, Plaintiffs' experts set out how the Health Information at issue is protected under federal and state law. As explained by computer scientist Dr. Zubair Shafiq, the Health Information is reasonably capable of being used to uniquely identify individuals. *See* Dkt. 42-4, Shafiq Decl. ¶¶ 15-21. This comports with the applicable definition for individually identifiable health information under HIPAA and personal information under California law, both of which are protected categories of information. Under HIPAA, individually identifiable health information is defined to be information created or received by a health care provider, related to past, present or future health condition or the provision of health care, which either (1) identifies the individual, *or* (2) for which there is a *reasonable basis* to believe the information *can be used* to identify the individual. *See* 45 C.F.R. § 160.103. By law, web URLs, IP addresses, account numbers, device identifiers, serial numbers, and *any other* unique identifying number, characteristic, or code are considered individually identifiable health information. *See* 45 C.F.R § 164.514(b)(2). Similarly, California protects "information that identifies, relates to, describes, is *reasonably capable of being associated with, or could reasonably be linked, directly or indirectly,* with a particular consumer or household." Cal. Civ. Code § 1798.140(v)(1), (aj) (emphasis added).[2]

The Health Information at issue meets both definitions. It contains device identifiers, IP address, cookies, pseudonyms, and "other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device that is linked to a consumer or household." CCAC ¶¶ 2, 34-36; Smith Decl. ¶ 58; Shafiq Decl. ¶¶ 15-21. Google is capable of associating, and does in fact associate, the Health Information at issue with individual patient identifiers. *See* CCAC

[2] Google attempts to confuse this issue by using varying phrases interchangeably: personally identify*ing* information, individually/personally identif*iable* information, *personal information,* and *protected health information*. Insofar as Google purports to give these terms a self-serving meaning inconsistent with applicable law, that meaning should be rejected. Plaintiffs' claims center on individually identif*iable* information and personal information when viewed as a whole. CCAC ¶¶ 34-36, 169.

§ IV.E. Specifically, Google can and does tie the Health Information it collects across different services to specific individuals. *See id.* ¶¶ 71, 83, 89, 91; Rebuttal Decl. of Dr. Zubair Shafiq ("Shafiq Reb. Decl.") ¶¶ 20-32.

B. GOOGLE'S MONETIZATION (I.E. USE) OF HEALTH INFORMATION

As alleged in the CCAC, Google leverages the Health Information for profit through its own marketing systems. *See* CCAC ¶¶ 111-42. In further support of these allegations, Plaintiffs' experts confirmed that the Health Information was used through Google's advertising systems.

Remarketing: Smith demonstrates that Google Source Code on Health Care Provider web properties transmitted patient identifiers, communications content, and Health Information to Google via the domain www.google.com/pagead/1p-user-list. *See* Smith Decl. ¶ 131 (showing transmission of Google Account ID, device identifiers, and content of communications with Mercy Health related to appointments, tests, and test results); *see also id.* ¶¶ 76, 80, 90, 93, 114, 127, 131, 134, 137, 142, 145, 148. Smith also demonstrates such transmissions to Google via the domain www.google.com/ads/ga-audiences. *See, e.g.*, Smith Decl. ¶¶ 100, 137. Both of these domains are associated with Google's ad server, Google Ads, and relate to remarketing services. *See, e.g.*, CCAC ¶¶ 74, 105-09, 111-42.

Conversions: Smith further demonstrates that Google uses the Health Information for conversion tracking. Specifically, Smith describes how Google re-directs patient identifiers, communications content, and personal health information to the following Google conversion tracking domains (1) adservice.google.com/ddm/fls/z, (2)fls.doubleclick.net, and (3) googleads.g.doubleclick.net/pagead/viewthroughconversion. *See, e.g.,* Smith Decl. ¶¶ 114, 124, 127, 134, 137, 142, 145, 148.

Further, evidence of Google's use can be found in Dr. Shafiq's Rebuttal Declaration, whose testing reveals that Google uses Health Information in its advertising systems, including personalized and targeted advertising. *See* Shafiq. Reb. Decl. ¶¶ 63-75.

C. GOOGLE DOES NOT PROTECT, PROHIBIT OR PREVENT THE TRANSMISSION AND USE OF HEALTH INFORMATION

Google impermissibly tries to insert its own version of the facts at issue, asserting that it

has "safeguards" against receiving Health Information (MTD at 6-8) in the form of policies that prohibit sharing Health Information with Google (MTD at 8-9), or using sensitive Health Information in personalized advertising (MTD at 9-10). But Google's rhetoric does not match reality. As shown by Plaintiffs' experts, Google's purported prohibitions do not stop Google from acquiring Health Information, or prevent the use of Health Information for purposes of advertising—personalized or otherwise.[3] *See* Smith Decl., *supra* (confirming data transmissions, including to Google advertising domains for user and audience lists); Shafiq Reb. Decl., *supra* (confirming use of Health Information for personalized advertising). Indeed, Google does not claim that any safeguards prevent it from creating internal remarketing or audience lists, user profiles, and otherwise leveraging Health Information once Google receives it.

Moreover, the specific examples of "safeguards" provided by Google are misleading. Google argues that the identifiers AdID, IDFA, Client IDs are "pseudonymous" and thus fall outside the applicable definitions of individually identifiable information and personal information. Not so. As noted above, Google can and does link the Health Information at issue, including these "pseudonymous" identifiers in a manner that is capable of, directly or indirectly, identifying an individual. *See supra* §§ III.A.2-.3. The use of the term "pseudonymous" is a misdirection that does not comport with applicable law. Google does not dispute identifiability of other identifiers alleged (*see, e.g.*, CCAC ¶¶ 34, 53, 58, 65, 77, 83, 89, 94, 100 (NID, IDE, DSID, _gid, _gcl_au, cid, gid,)), and shown in the Smith Declaration (*see, e.g.,* Smith Decl. ¶¶ 56, 100, 127, 138). Also of no help are user Settings (*e.g.* WAA, sWAA, NAC) because they do not address Google's *collection* of Health Information; they only pertain, at most, to the delivering of personalized ads. Further, these settings engage in "dark patterns" that intentionally obfuscate and confuse their true purpose so that Google can collect the information at issue. *See* Shafiq Reb.

[3] Google restricts its discussion to *personalized advertising*. But Plaintiffs' allegations are not so limited, and a showing that Google uses protected data for "personalized advertising" is not a required element of every claim. Moreover, there *is evidence* of use for personalized advertising. *See supra* § III.B (discussing transmissions to Google's remarketing and conversation sites, both of which are common tools for personalized advertising); Zervas, *et al.*, *Understanding Emerging Threats to Online Advertising,* at 2. Boston U. Sch. of Mgmt. Rsch. paper No. 2505643 (June 11, 2016), at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505643 (retargeting is "a common implementation of ad tracking technology" which permits "personalized ads across the web").

Decl. ¶¶ 18-19 (explaining the manipulative design employed by Google and referencing publicly filed Google documents that agree that the WAA settings are misleading as they "imply we [Google] don't log the data, but obviously we do").[4]

Google also claims that it "proactively prevents" misuse of sensitive information because "Sensitive" websites (*e.g.*, plannedparenthood.org, keckmedicine.org, memorialcare.org, medstarhealth.org, gundersenhealth.org, mercy.net, altonmemorial.org, *see* Dkt. 48-24, Takabvirwa Decl., ¶ 7) cannot engage in personalized advertising vis-à-vis advertiser-curated audience lists or remarketing lists. *See* MTD at 10 *citing* Takabvirwa Decl. ¶ 10. This claim is false. Smith shows that Health Information was transmitted to Google's from "Sensitive" websites: MedStar (Smith Decl. ¶¶ 112-14), Mercy (*id.* ¶¶ 115-21), Gundersen Health (*id.* ¶¶ 122-31), Planned Parenthood (*id.* ¶¶ 135-39); Keck Medicine (*id.* ¶¶ 140-42), MemorialCare (*id.* ¶¶ 143-45), and Alton Memorial (*id.* ¶¶ 153-61). This includes transmissions to Google ad servers for remarketing and conversion tracking. *See* § II.B. If, as claimed, "Sensitive" websites are prevented from using its tools for personalized advertising, these transmissions to remarketing and conversion tracking domains would not occur.

IV. CIVIL LOCAL RULE 7-3(a) AND (c) EVIDENTIARY OBJECTIONS

1. The Zervas Declaration Is Unreliable

The Court should strike portions of the Zervas Declaration on the following grounds:

First, the Zervas declaration contains numerous improper legal conclusions regarding whether Google "intercepted" communications, whether Google and Health Care Providers are legally responsible, interpretation of HIPAA rules, and consent. *See U.S. v. Tamman*, 782 F.3d 543, 552-53 (9th Cir. 2015) ("an expert cannot testify to a matter of law"); *see, e.g.,* Zervas Decl. ¶¶ 14, 62, 65-66, 69, 79, 85-86, 120, 126.

Second, the Zervas declaration merely regurgitates self-serving facts given to Zervas by other Google declarants – without any additional analysis or investigation by Zervas – leading to numerous speculative assertions. *See Dep't of Toxic Substances Control v. Technichem, Inc.*, 2016

[4] The Zervas Declaration also addresses certain methods that he claims users could use to stop the transmission of their Health Information (*see* Zervas Decl. § IV.C). These methods do not work as claimed. *See* Rebuttal Decl. of Richard Smith ("Smith Reb. Decl.") ¶¶ 6, 8-40.

WL 1029463, at *1 (N.D. Cal. Mar. 15, 2016); *see, e.g.,* Zervas Decl. ¶¶ 16-17, 26-27, 31, 36, 40, 43, 49, 53, 55-56, 61, 66-69, 75-78, 80-84, 87, 97, 127, 134-36, 140. The Zervas declaration also recites irrelevant information, like recitation of Health Care Provider statements. *See* Fed. R. Evid. 702; *Daubert v. Merrell Dow Pharms., Inc.*, 509 U.S. 579, 591 (1993) ("testimony which does not relate to any issue in the case is . . . non-helpful"); *see, e.g.* Zervas Decl. ¶¶ 93-96, 109-11.

Third, the Zervas declaration contains unreliable opinions because the underlying testing did not use reliable methodology that would survive peer review, as Plaintiffs' expert Dr. Shafiq explains. *See Metabyte, Inc. v. Canal+ Techs., S.A.*, 2005 WL 6032845, at *6 (N.D. Cal. June 17, 2005) (excluding expert due to unreliable methodology); Shafiq Reb. Decl. ¶¶ 33-41; *see, e.g.*, Zervas Decl. ¶¶ 99-102.

Fourth, Zervas' analysis is suspect because he contradicts his prior testimony in other litigation and his own prior peer-reviewed research. For example, Zervas opines here that "the user's choice of browser will impact data transmissions to Google domains." Zervas Decl. ¶ 103. But Zervas testified in *Calhoun v. Google* that the same Google services at-issue here are "browser-agnostic," meaning that, when he tested "different browsers, I saw the same transmissions. So to me, this is browser-agnostic." Supp. Decl. Jay Barnes ("Barnes Supp. Decl.") ¶ 16. By way of background, Zervas made his browser-agnostic statement in support of Google's overarching claim in *Calhoun* that its source code was intended to work with all browsers, an argument on which Google prevailed. *See id.* ¶ 12-13. Likewise, here, Zervas criticizes Plaintiffs' expert Dr. Libert, and disputes Dr. Shafiq's conclusion that the data is personally identifiable. But in a 2016 peer-reviewed research publication, Zervas relied on Libert's work (which employed the same methodology used in this action) to support his conclusions, including that "user IDS can usually be linked to names, addresses and other personally identifying information," and the linking of small trackers to large entities "introduces further privacy and security concerns." *See* Barnes Supp. Decl. ¶¶ 10-11.

2. The Teehan Declaration Is Unreliable

Plaintiffs move to strike the Teehan declaration (Dkt. 48-47) in its entirety because Teehan purports to opine on the benefits of GA to Health Care Providers and Health Care Providers'

responsibilities relating to the privacy of patients' information but provides *no* factual basis or methodology for these opinions. For instance, Paragraphs 11, 12, 19, 25, 29, and 32 speculate on the subjective intent and experiences of all Health Care Providers, which neither Teehan nor any other expert can reliably opine upon. Further, Teehan offers conclusory and unsupported opinions concerning the impact of GA on the provision of health care, patient privacy, and health care costs, without citing any costs analysis, study, or other factual basis. *Id.* ¶¶ 10, 13, 15, 16-19, 28, 31, 32. Otherwise, Teehan merely restates HIPAA requirements, Google's web pages, and other sources without elaboration. *See id.* ¶¶ 14, 16, 19-22, 26, 27. These are insufficient bases to assert expert testimony as discussed above. *See Technichem, Inc.*, 2016 WL 1029463; *Ollier v. Sweetwater Union High Sch. Dist.*, 768 F.3d 843, 861 (9th Cir. 2014) (excluding testimony based on "personal opinions and speculation").

V. ARGUMENT

A. MOTION FOR PRELIMINARY INJUNCTION

As set forth in Plaintiffs' moving brief, the applicable standard of review is that of a prohibitory injunction but, even if viewed under the heightened standard of a mandatory injunction, Plaintiffs still meet the standard for relief. *See* MPI at 8.

1. Plaintiffs Have Article III Standing for Injunctive Relief

Evidence of Injury: Plaintiffs seek injunctive relief for Google's violations of the ECPA, CIPA, and UCL, and for intrusion upon seclusion. Contrary to Google's argument that Plaintiffs must show how Google "used" their information, Plaintiffs need not show injury beyond the harm to the substantive privacy rights that the statutes protect. *See In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 598 (9th Cir. 2020) ("*FB Tracking*") (ECPA and CIPA); *Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1117-18 (9th Cir. 2020) (UCL, ECPA, and CIPA). The same is true for Plaintiffs' common law invasion claim, which "do[es] not always require additional consequences to be actionable." *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017); Rest. 2d Torts § 652B ("The intrusion itself makes the defendant subject to liability"); *Brown v. Google, LLC*, 2023 WL 5029899 at *5 (N.D. Cal. Aug. 7, 2023); *cf. Hancock v. Urban Outfitters*, 830 F.3d 511, 514 (D.C. Cir. 2016) ("bare" *procedural* violation of consumer protection statute)

(cited by Google). Google also presents a false narrative in discussing only the harm from GA. *See* MTD at 16. Plaintiffs *absolutely* allege, and show, that Google uses their Health Information for other products. *See* § III.A.1 (products at issue are beyond GA); § III.B (monetization of information). Further, GA is not merely an "analytics service." It is a marketing service that serves as a fulcrum between Google's many other products to commingle, aggregate and populate user profiles for marketing purposes. *See* CCAC ¶¶ 119-95.

Google Received Health Information: Plaintiffs' motion is replete with evidence of Google's unlawful collection of Health Information, which includes information that is defined as individually identifiable health information under HIPAA and protected personal information under California law. Google's argument that Plaintiffs "provide no evidence that Google received any PII that could risk an injury-in-fact" is simply wrong. *See* MTD at 16. Google relies on its own self-serving definition of what "PII" and "PHI" can comprise, but as discussed *supra* § III.A.3, the applicable definition of identifi*able* and *personal information* require only the *reasonable capability* of identification, and not proof of an actual identification. Contrary to Google's claims that Google's linking and identification of data are speculative (*e.g.*, MTD at 29), Google has acknowledged (when in its interest to do so) that Google can and does link various identifiers and information together after receiving Health Information, including linking Google's GAIA ID (a unique identifier associated with individual Google accounts) with device identifiers (*e.g.*, NID, IDE, and DSID, used to facilitate advertisements). *See* Shafiq Reb. Decl. ¶¶ 20-32.

Plaintiffs' allegations and evidence that Google can and does link identifiers undermine Google's arguments regarding the "identifiability" of specific pieces of data at issue, including as pertains to Plaintiffs' standing. *See, e.g.*, MTD at 7. For example, Google asserts that AdID, IDFA, and Client IDs are not identify*ing* because they are "neither tied to a user's identity nor used to personally identify a user." *Id.* Aside from ignoring the relevant definitions (which speak to reasonable capability of identification, i.e., identifi*ability*), the factual assertion that these identifiers are not "used to identify a user" is incorrect. Google does, in fact, tie AdID, IDFA, and Client IDs to *other identifiers* (*e.g.*, Biscotti ID and Zwieback ID) to facilitate identification and ad placement. *See* Shafiq Reb. Decl. ¶¶ 20-32. Likewise, Google incorrectly states that the _ga

cookie cannot, by itself, be used to track users across different websites. *See* Dkt. 48-1; Ganem Decl. ¶ 35. In truth, the _ga cookie is a unique value that Google transmits in a "cid" or "Client ID" parameter. *See* Smith Decl. ¶¶ 59, 70-72. Google has acknowledged, in other litigation, that it links the Client ID to other identifiers, like the Google Analytics User ID and IDE (used to target individuals for Google Display Ads). *See* Shafiq Reb. Decl. ¶¶ 20-32. Google, in turn, links IDE to, among other things, GAIA ID (which is the unique identifier for an *individual's* Google account). *See id.* And, in turn, Google links the GAIA ID to dozens of other identifiers. *See id.* The continuous and overlapping linking of identifiers ensures that even purportedly pseudonymous information is eventually linked to an individual identifier. In any event, even purportedly anonymous tracking can be sufficient for Article III. *See e.g., Brown*, 2023 WL 5029899 at *5 (rejecting argument that privacy harm is not concrete where only anonymized data is collected) *citing Campbell*, 951 F.3d at 1112. Google's reliance on *Dinerstein v. Google LLC* is misplaced, as the facts are vastly different. *Dinerstein* involved a research partnership between Google and one hospital, wherein the hospital transferred de-identified medical records to Google and Google contractually agreed that it would not attempt to re-identify the data. 73 F.4th 502, 502-03 (7th Cir. 2023). *Dinerstein* is the inverse of Plaintiffs' claims, which involve Google's collection of Health Information for the purpose of identifying patients for use in advertising services.

In addition to disputing the identifiability of Health Information at issue by redefining it and otherwise ignoring the evidence, Google also argues that it does not receive Health Information because it has policies. *See* MTD at 16. That is not true because Plaintiffs offer uncontroverted proof that data transmission to Google occur. *See* Smith Decl. ¶¶ 61 *et seq.*

Fairly Traceable to Google: Plaintiffs adequately allege, and show, that their injuries are fairly traceable to Google. Google tries to shift responsibility to Health Care Providers (MTD at 17), but Judge Orrick rejected a similar argument in *In re Meta Pixel Healthcare Litig.*, explaining: "[t]hat website developers may also be liable does not mean, of course, that Meta is exempt from liability." 2022 WL 17869218, at *19 (N.D. Cal. Dec. 22, 2022). This was particularly true, given Meta's concession "that it 'has the ability to block all data coming in from a specific website'" and thus, "is capable of turning … off" inappropriate data flow "for certain websites." *Id.* The same

applies here. The wrongful conduct of others does not absolve Google. And, like Meta, Google's concessions regarding its ability to stop the unlawful data flow discredits its traceability argument. *See* Takabvirwa Decl. ¶¶ 23-24 ("Google may suspend an advertiser's Google Ads account after one or more violations of the Advertising Policy"). Google's claim that Plaintiffs seek relief under HIPAA is also obviously wrong. *See* CACC, Counts 1-14; MPI at 1.

Continued Harm: Plaintiffs demonstrate "continuing, present adverse effects" as required on this motion. *Brown,* 2023 WL 5029899 at *7 *citing City of Los Angeles v. Lyons*, 461 U.S. 95, 102 (1983). Google argues Plaintiffs cannot show "that they will be wronged again in a similar way" because they submitted declarations that they "no longer use the Websites and will not use them in the future." MTD at 17. But Google still has their information and should not. Moreover, Google's conduct prevents Plaintiffs from exchanging confidential communications with their Health Care Providers through their devices, including smartphones, that the Supreme Court has explained are "indispensable to participation in modern society." *Carpenter v. U.S.*, 138 S. Ct. 2206, 2220 (2018) *citing Riley v. California*, 573 U.S. 373, 385 (2014).

2. Google Cannot Demonstrate Valid Consent

As set forth in Plaintiffs' Motion for Preliminary Injunction, Google bears the burden of proving consent. MPI at 9. Google expressly promised that it would not collect Health Information absent a limited set of circumstances not applicable here, and cannot prove consent with respect to conduct that it *promised not to engage in*. *See id.* at 9-11 *citing* Google Privacy Policy; *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1066 (N.D. Cal. 2021) (no consent where Google's "statements suggest that a user's activity in private browsing mode is not saved or linked to the user"); *Calhoun v. Google*, *LLC*, 526 F. Supp. 3d 605, 621 (N.D. Cal. 2021) (no consent because Google's privacy notice "makes specific representations that could suggest to a reasonable user that [defendant] would not engage in the alleged data collection"); *FB Tracking*, 956 F.3d at 603 ("the critical fact was that the online entity represented to the plaintiffs that their information would not be collected, but then proceeded to collect it anyway").

Google claims that its own Privacy Policy somehow establishes consent (MTD at 18), but fails to identify where or how the precise conduct at issue was disclosed. Courts routinely reject

such arguments, even where (unlike here) the defendant tries to support them. *See McCoy v. Alphabet, Inc.*, 2021 WL 405816, at *6 (N.D. Cal. Feb. 2, 2021) (holding Google's statement regarding "[A]ctivity on third-party sites and apps that use our services" would not be "understood by a reasonable user to disclose collection of [data] on an independent third-party [web property]."); *Calhoun,* 526 F. Supp. 3d at 621.

Nor can Google establish consent by pointing to Health Care Providers' privacy policies. *First*, under HIPAA, Health Care Providers cannot obtain consent to disclose or use patients' Health Information for advertising via browser-wrap agreements like those Google cite. Thus, there is no patient consent. *See* MPI at 8. On this point, Google argues only that there is "no evidence that the Websites sent Google [Protected Health Information] in contravention of Google's restrictions." MTD at 18. Incorrect. That evidence is in the record as discussed above. *See* § III.A. Even if Google had a policy for Health Care Providers to "disclose their use of . . .GA" as it claims (MTD at 18),[5] it is clear that such disclosure did not address the specific conduct at issue here, failing to address, among other things, illicit conduct in patient portals and Google's subsequent use of the information for advertising purposes. Moreover, a review of Google's recommend GA disclosure shows that Google prompts Health Care Providers to include a hyperlink to a web page, which, in turn incorporate the Google Privacy Policy. *See* Barnes Supp. Decl. ¶¶ 7-8. Consequently, Google's attempts to escape its own promises are unavailing. All roads lead back to the Google Privacy Policy. The Health Care Providers' policies are thus irrelevant as discussed herein and in Plaintiffs' Opposition to Google's Request for Judicial Notice.

Second, whatever consent Health Care Providers did (or did not) obtain relating to *their* collection of data cannot—by proxy—establish consent for *Google* to track, collect, use, and store Plaintiffs' and class members' Health Information. *See* MPI at 8-11; *In re Pharmatrak, Inc.*, 329 F.3d 9, 21 (1st Cir. 2003) (website's implementation of defendant's technology did not provide proxy consent for collection of users' personal information and users themselves did not consent when website did not mention "collection of personal information by a third party"); *In re Google Inc.*, 2013 WL 5423918, at *13 (N.D. Cal. Sept. 26, 2013) (disclosures about interception "under

[5] Which argument, on its face, applies only to GA.

a different set of circumstances" do not create consent); *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1072 (N.D. Cal. 2016) (only consent "to the particular conduct" is effective). The reasonable consumer standard applicable here need not look past Google's "misleading representations" that it would not collect Health Information contained in its own Privacy Policy. *See Williams v. Gerber Prods. Co.*, 552 F.3d 934, 939 (9th Cir. 2008). At best, users would have no way of deciphering between the conflicting statements about what data collection practices Google actually engages in. Google cannot establish consent by confusion. *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 789 (N.D. Cal. 2019) ("*FB Cons. Priv.*") (if the "language at issue is reasonably susceptible to more than one interpretation, with one of those interpretations suggesting consent and another belying it, the Court cannot decide the consent issue in [Defendants'] favor[.]"). Google's authority do not deal with attempts to impute consent via third-party statements. *See Matera v. Google*, 2016 WL 5339806, at *7 (N.D. Cal. Sept. 23, 2016) (analyzing Google policies); *Calhoun,* 526 F. Supp. 3d 605 (same); *Snipes v. Wilkie*, 2019 WL 1283936, at *7 (N.D. Cal. Mar. 20, 2019) (dismissing claim that supervisor invaded privacy where plaintiff made purportedly private phone call in defendant's presence).

Third, Google does not dispute that there is *no consent* with respect to the tracking and collection occurring within authenticated pages, *e.g.*, patient portals.

3. Plaintiffs Sufficiently Pled and Are Likely to Prevail on the ECPA, CIPA, UCL, and Privacy Claims

Plaintiffs predicate their MPI on claims under the ECPA, CIPA, and UCL, and for intrusion upon seclusion. Plaintiffs adequately support each of these claims and, as discussed in Plaintiffs' moving brief and further below, Plaintiffs will likely succeed on the merits of each of these claims.

a) The ECPA Claim

One-Party Consent: Plaintiffs allege that any purported consent Google received from Health Care Providers to obtain Plaintiffs' and class members' Health Information was not valid. *See* CCAC ¶ 326. Google argues that consent by Health Care Providers to GA is sufficient to defeat Plaintiffs' ECPA claim. This argument fails on two grounds.

First, Google fails to present proof that it obtained consent from Health Care Providers, as

is its burden. The mere use of Google's products is not sufficient. *See In re Pharmatrak, Inc.*, 329 F.3d at 19-20 (rejecting proposition that use of a service is consent to all subsequent conduct; "a reviewing court must inquire into the *dimensions of the consent* and then ascertain whether the interception exceeded those boundaries"). Google offers no evidence that Health Care Providers consented to GA to facilitate Google's tracking, collection and use of patient Health Information. And Google provides no basis for consent regarding any other Google product. Google's consent argument should be rejected on this ground alone.

Second, even if Health Care Providers allowed it, Google's conduct on their websites is still tortious in violation of the ECPA, which imposes liability where, as here, the "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." CCAC ¶ 327; 18 U.S.C. § 2511(2)(d). This applies where a recording is "done for the purpose of facilitating some further impropriety" (*U.S. v. McTiernan*, 695 F.3d 882, 889 (9th Cir. 2012)), and holds true even if there may have otherwise been a lawful purpose for the recording. *See Sussman v. ABC, Inc.*, 186 F.3d 1200, 1202 (9th Cir. 1999). The mere existence of a lawful purpose cannot "sanitize a [recording] that was also made for an illegitimate purpose; the [recording] would violate section 2511." *Id.* An illegitimate purpose may include recording to invade a plaintiffs' privacy or defraud a plaintiff, or unfair business practices. *See Detesera v. Am. Broad. Cos., Inc.*, 121 F.3d 460, 467 n.4 (9th Cir. 1997). Courts have also found Section 2511(2) satisfied where, as here, plaintiffs allege intent to commit trespass, violate state computer crime laws, or commit common law privacy torts. *See, e.g., Brown,* 525 F. Supp. 3d at 1067 (CDAFA, intrusion upon seclusion, and invasion of privacy); *Planned Parenthood Fed'n of Am., Inc. v. Ctr. For Med. Progress*, 214 F. Supp. 3d 808, 828 (N.D. Cal. 2016) (invasion of privacy); *Med. Lab. Mgmt. Consultants v. Am. Broad. Cos., Inc. v. ABC, Inc.*, 1997 WL 405908, at *2 (D. Ariz. Mar. 27, 1997) (trespass). All apply here.

Interception: Google argues that it did not "intercept" communications because it merely provided a tool for websites to record user interactions. *See* MTD at 20. This argument misstates the facts and the law. On the facts, as Plaintiffs' experts show and the CCAC alleges, Google is not merely providing a tool for recording but rather actively acquiring and using patients' Health

Information and contents of communications for its own purposes and gains. *See* Smith Decl. ¶¶ 93, 100, 114, 117, 121, 124, 127, 131, 134 (documenting transmissions of identifiers and electronic communications, including to Google remarketing and conversion domains); CCAC ¶¶ 4-8, 37-167; *see Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503 (C.D. Cal. 2021) (separate entity providing software as a service not excluded from liability merely because recording was at direction of, or for benefit of one of the parties to communication); *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051 (N.D. Cal. 2015) (interception alleged where carried out by third-party software); *see also FB Tracking*, 956 F.3d at 608 ("the Wiretap Act's legislative history evidences Congress's intent to prevent the acquisition of the contents of a message by an unauthorized third-party or 'an unseen auditor.' Permitting an entity to engage in the unauthorized duplication and forwarding of unknowing users' information would render permissible the most common methods of intrusion").

On the law, Google ignores the ECPA's definition of "interception," which is simply the "acquisition of the contents of … a[n] electronic … communication." 18 U.S.C. § 2510(4). As noted above, Google's collection and use of patient Health Information and electronic communications amply demonstrate that Google in fact *acquired* the contents of Plaintiffs' and class members' electronic communications. *See* § III.A-C. Further, Google's reliance on *Graham v. Noom* and *Williams v. What If Holdings, LLC* is misplaced. As Google recognizes, those cases turn on whether the defendant acted in merely a storage capacity or acquired information for its own uses and gains. *See* MTD at 20 (distinguishing factor in *Noom* was whether defendant "aggregated the data for resale or that it used the data itself") (cleaned up); *see also* MTD at 20 (key factor in *Williams* was the distinction between "routine documentation" as opposed to "data mining"); *Katz-Lacabe v. Oracle Am., Inc.*, 2023 WL 2838118, at * 9 (N.D. Cal. Apr. 6, 2023) (distinguishing *Noom* where defendant had used the data). Here, Plaintiffs have alleged, and proven, that Google actively tracks, re-directs and collects Health Information via the Google Source Code (*see* § III.A.2), and that, upon receipt, Google then links, associates and aggregates that information in furtherance of its advertising systems (*see* § III.A.2, III.B).

Intent: Plaintiffs adequately plead Google's intent. *See* CCAC ¶ 318. They need only show Google's acts were "'done on purpose,' even if that purpose was not nefarious and [Google] was

unaware that the use was unlawful." *Bliss v. CoreCivic, Inc.*, 580 F. Supp. 3d 924, 929 (D. Nev. 2022) *quoting U.S. v. Christensen*, 828 F.3d 763, 774-75 (9th Cir. 2015). Intent is satisfied where, as here, Google is aware that its product is recording information that it should not. *See In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 815 (N.D. Cal. 2020); *Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1044 (N.D. Cal. 2014). Facts supporting Google's intent include unrebutted evidence that it receives and uses the information at issue (§§ III.B, C) and thus must know what information it receives (sufficient on its own) *and* knows it should not receive protected information, evidenced by the lip service Google pays to the illegality of such conduct while secretly and simultaneously reaping the benefits of the illicit data flow. Contrary to Google's arguments (MTD at 21-22), this conduct falls squarely within the intent element as guided by the above cases, and common sense.

b) The CIPA Claim

The elements of a CIPA claim overlap significantly with the ECPA, and thus, for the same reasons stated above, Plaintiffs have adequately alleged and proven the elements of interception and intent. In addition, Google makes two CIPA-specific arguments, which are addressed below.

Within the State of California: Google is a California entity, with headquarters in the State of California, and Google planned and carried out its scheme to intercept communications from the state of California. *See* CCAC ¶ 12. Nonetheless, Google argues that Plaintiffs have not adequately alleged that at-issue communications were "sent from or received at any place" in California. *See* MTD at 23 *quoting* Cal. Penal Code § 631. According to Google, this element of § 631 (not present in § 632) cannot be satisfied because most of the Plaintiffs, and their Health Care Providers, reside in other states. Google's reasoning misconstrues CIPA, which does not grant California entities like Google unlimited license to intrude on communications if there is some out of state component. *See* Cal. Penal Code § 631(a) (interception occurs "while" the communication is "pass[ed] over any wire, line, or cable, or is being sent from, or received at any place within this state."). Courts thus unambiguously recognize that this law applies where (as here) "the Complaint asserts CIPA claims against a California defendant for alleged conduct that occurred in California." *Carrese v. Yes Online, Inc.*, 2016 WL 6069198, at *4 (C.D. Cal. Oct. 13,

2016) (citing cases).

Confidential Communications under Penal Code § 632: Plaintiffs' allegations that they have a reasonable expectation of privacy, and thus confidentiality, in their Health Information and communications are factually supported. *See* CCAC ¶¶ 196-254, 343. Google's argument that statements on Health Care Provider websites negate that expectation (MTD at 23) lacks merit for the reasons set forth above. *See* § V.A.2; CCAC, ¶¶ 196-266; *In re Meta Pixel*, 2022 WL 17869218 at *15 (finding "objectively reasonable expectation that [plaintiffs'] communications with their medical providers were confidential based on the laws and regulations protecting the confidentiality of medical information").

c) The Privacy Claims

Specificity as to Plaintiffs: In addition to the above meritless arguments regarding Google's intent and Plaintiffs' reasonable expectation of privacy, Google argues that Plaintiffs fail to plead with specificity what Google unlawfully obtained from each Plaintiff. *See* MTD at 24. This assertion is belied by the CCAC itself, which sets forth detailed and specific allegations as to the Health Information at issue. *See* § III.A.2 Plaintiffs' pleadings are supported by the Smith Declaration, which confirms that the alleged data points are, in fact, transmitted to Google via the Google source code. *See id.* These allegations and unrebutted proof are more than sufficient to demonstrate the tracking and collection of personal information, including highly private and protected health information.

Further, and contrary to Google's assertions, more specific allegations as to the precise data obtained regarding each individual Plaintiff is not required. The Ninth Circuit has held that plaintiffs may pursue their claims without identifying specific communications at issue where plaintiffs describe the network of surveillance affecting them, the technical means used to receive the diverted communications, the particular electronic communications equipment used and their location, and the specific entity through which the communications were intercepted. *See Jewel v. Nat'l Sec. Agency*, 673 F.3d 902, 906 (9th Cir. 2011); *see also ACLU v. Clapper*, 785 F.3d 787, 796 (2d Cir. 2015); *Schuchardt v. POTUS*, 839 F.3d 336, 346 (3d Cir. 2016). Google's cited cases are inapposite or contrary to Ninth Circuit precedent. *Hammerling* involved Google's collection

of app usage information where plaintiffs did not identify any specific "content" at issue. *Kurowski* and *Cousin* conflict with *Jewel*. In fact, Google's argument on this point has already been rejected by courts in this District. *See, e.g.*, *In re Google RTB Consumer Priv. Litig.*, 606 F. Supp. 3d 935, 942-43 n.5 (N.D. Cal. 2022) (rejecting Google's argument for specificity: "the Court finds these arguments specious for a Rule 12 motion based solely on the need to provide notice pleading under Rule 8, and Google's significant advantage and control of the information at issue"); *Valenzuela v. Nationwide Mut. Ins. Co.*, 2023 WL 5266033, at *5 (C.D. Cal. Aug. 14, 2023) (factual allegations that defendant was capable of intercepting messages and plaintiff sent messages sufficiently specific); *see also FB Cons. Priv.*, 402 F. Supp. 3d at 787 (holding requirement for "specific allegations about which app developers or business partners obtained which plaintiffs private information … puts too great a burden on the plaintiffs, at least at the pleading stage (and probably at any stage)").

Google Is not an Authorized Recipient: Google argues that it is "an authorized recipient" of the Health Care Providers and, therefore, no intrusion occurred. *See* MTD at 25. However, there is no single-party "consent" defense to invasion of privacy claims.

Receipt of Personal Information: Google argues that there is no evidence that it received "PII or PHI" from the Healthcare Provider properties. *See* MTD at 26-27. This argument misstates the allegations and employs an incorrect definition of PII and PHI. *See* § III.A.2. As to the Health Information at issue, Google ignores the Smith Declaration, the Shafiq Declaration, and public court filings in other cases involving Google's data collection systems, all demonstrating that the information is reasonably capable of being used to identify an individual or household. *See* § III.A.2. Further, Google's insistence that Client ID, AdID, and IDFA can only be the subject of a privacy claim "if they are linked with an identifiable person" is legally incorrect. These IDs are device identifiers covered under both state and federal definitions of identifiable information because Google *is* reasonably capable of linking the above identifiers to other information that can, directly or indirectly, identify an individual. *See* 45 C.F.R § 164.514(b)(2); Cal. Civ. Code § 1798.140(v)(1); (aj)); Shafiq Reb. Decl. ¶¶ 20-32.

Likewise, Google's reliance on purported "user controls" (*i.e.,* WAA, sWAA, NAC) for

the proposition that users can (or should have to) prevent the transmission of certain information should be rejected. But these "controls" are presented to users in a manner intentionally designed to subvert user consent and choice. *See Brown*, 2023 WL 5029899 at *7 (express consent requires "disclosures [that] 'explicitly notify' users of the practice at issue"); Shafiq Reb. Decl. ¶¶ 17-19.

Highly Offensive Conduct: Plaintiffs have alleged and proven that Google created surveillance systems to collect massive amounts of Health Information, which is highly offensive. *See* CCAC ¶ 356. In fact, the Google Source Code is present on approximately 6,046 Health Care Provider web properties (*see* CCAC ¶ 143; Libert Decl. ¶¶ 16-19, 23), and it results in the re-direction of an alarming amount of Health Information—including information *within patient portals*—to Google. *See* CCAC ¶¶ 34-36; Smith Decl. ¶¶ 107 *et seq.* Upon receipt, Google has unfettered ability to associate, aggregate, and use the information to profile users and facilitate its own marketing. *See* § III.B. Google contends otherwise (MTD at 27), but points to no legal support. The conduct at issue is objectively highly offensive conduct. *See In re Meta Pixel*, 2022 WL 17869218 at *16 (rejecting same argument by Meta in case regarding health information: "Meta does not point to a single case where a court found that the collection of the kinds of information at issue here did not constitute a highly offensive invasion of privacy"); *see also Katz-Lacabe.*, 2023 WL 2838118, at * 7-8 (upholding privacy claims in part due to collection of "vast repository of personal data" including health information; noting "determinations of the egregiousness of the privacy intrusion are not usually resolved at the pleading stage"); *McDonald v. Kiloo ApS*, 385 F. Supp. 3d 1022, 1034-35 (N.D. Cal. 2019) (allegations that "data was secretly collected, how the collection was done, and how the harvested data was used" support offensiveness element at pleading stage).

d) The UCL Claim

Plaintiffs' allegations of a cognizable injury under the UCL are well pled. Plaintiffs' loss of control over their Health Information through Google's deception constitutes at least two of the "innumerable ways in which economic injury from unfair competition may be shown" under state law, including because plaintiffs "have a present or future property interest diminished" and "surrender[ed] in a transaction more" than they otherwise would have. *Kwikset Corp. v. Superior*

Ct., 51 Cal. 4th 310, 323-24 (2011) ("the quantum of lost money or property necessary to show standing is only so much as would suffice to establish [Art. III] injury in fact."); § V.A.1.

Google disputes Plaintiffs' allegations, and tries to discredit authority supporting them (MTD at 28), but Judge Koh correctly applied California law in *Calhoun*, a case concerning much of the same information that is at issue here: unique identifiers, web browsing history, and content of communications, in holding that the loss of personal information established "economic injury" including deprivation of a "property interest." 526 F. Supp. 3d at 613; CCAC ¶¶ 33-36. Judge Koh reasoned that these losses constituted "economic injury" under both Article III and California's UCL, consistent with federal appellate authority. *Reid v. Johnson & Johnson*, 780 F.3d 952, 958 (9th Cir. 2015) (UCL "demands no more than the corresponding requirement under Article III of the U.S. Constitution."); *FB Tracking*, 956 F.3d at 599 (personal information suffices to establish "economic injury" for constitutional standing purposes); *see also Brown v. Google*, LLC, 2021 WL 6064009, at *17 (N.D. Cal. Dec. 22, 2021) (approving *Calhoun's* reasoning). Judge Koh's analysis also respects legislative intent. The UCL's standing requirement was never intended to diminish consumers' rights to bring claims for conduct directly affecting their own property interests and privacy rights; it was enacted to "curtail the prior practice of filing suits on behalf of clients who have not used the defendant's product or service, viewed the defendant's advertising, or had any other business dealings with the defendant." *Hinojos v. Kohl's Corp.*, 718 F.3d 1098, 1104 (9th Cir. 2013) (citations omitted).

Plaintiffs recognize that some district courts have reached different conclusions about certain theories of injury based upon personal data, but even if Article III standing is "different from UCL standing," as those cases emphasize, cognizable injuries under both standards can overlap. *See* MTD at 28-29 & n.11. None of Google's authority explains why the economic injury arising from deprivation of property—recognized in *FB Tracking*—would not satisfy the UCL. Instead, *Cottle v. Plaid Inc.* focused on money, rejecting the theory that app users "surrendered more" in transactions with the defendant because "Plaintiffs do not allege that they paid any money." 536 F. Supp. 3d 461, 484 (N.D. Cal. 2021); *see also Wesch v. Yodlee, Inc.*, 2021 WL 1399291, at *6 (N.D. Cal. Feb. 16, 2021) ("because Plaintiffs have not paid [defendant] any money

. . . Plaintiffs have not alleged how they lost money or property.") Similarly, *Adkins v. Facebook, Inc.* concerned a theory of "lost value" of information, not lost property. 2019 WL 3767455, at *3 (N.D. Cal. Aug. 9, 2019).

Plaintiffs' Diminished Property Interest Is Well Pled: As the Ninth Circuit has recognized, California defines property very broadly: "The ownership of a thing is the right of one or more persons to possess and use it to the exclusion of others. . . . The thing of which there may be ownership is called property." *G.S. Rasmussen & Assocs. v. Kalitta Flying Serv.*, 958 F.2d 896, 902 (9th Cir. 1992) *quoting* Cal. Civ. Code § 654; *see also Fields v. Michael*, 91 Cal. App. 2d 443, 449 (1949) ("[t]he word 'property' may be properly used to signify any valuable right or interest protected by law"). The exclusivity inherent in a property right extends to unauthorized copying and subsequent use of property. "[A]lthough the owner may retain possession of the original property, there has been nevertheless a deprivation of property when a copy is made and retained by another." *People v. Kwok*, 63 Cal. App. 4th 1236, 1251 (1998) (explaining such taking "is analogous to making . . . an unauthorized copy of computer data."); *CTC Real Est. Servs. v. Lepe*, 140 Cal. App. 4th 856, 860-61 (2006) ("[o]ne's personal identifying information can be the object of theft" and "is a valuable asset") cited with approval in *FB Tracking*, 956 F.3d at 600.

Here, as in *Calhoun*, Plaintiffs allege both an impairment of a property right and an interest protected by law. Google treats *Plaintiffs*' data as though it is *Google's* data and uses it for whatever purposes Google sees fit. If the Court is inclined to require lost "money" as some others have done, Plaintiffs support that theory as well, by demonstrating that a market for their data exists, *i.e.*, it has financial value. *See* CCAC ¶¶ 272-93, 381, 382. Similar pleadings have been found sufficient. *See In re Facebook Priv. Litig.*, 572 F. App'x 494, 494 (9th Cir. 2014) (plaintiffs plausibly alleged lost sales value of personal information)*; see also Callahan v. PeopleConnect, Inc.*, 2021 WL 5050079, at *19 (N.D. Cal. Nov. 1, 2021); *Brown v. Google*, 2023 WL 5029899, at *21 (lost CCPA "property interest"). Many courts recognize that theft of personal information constitutes economic loss. *See, e.g.*, *In re Anthem, Inc. Data Breach Litig.*, 2016 WL 3029783, at *15 (N.D. Cal. May 27, 2016); *Doe v. Virginia Mason Med. Ctr.*, 2020 WL 1983046, at *1 (Wash. Super. Feb. 12, 2020) (recognizing property right in healthcare identification data). As for

impairment of a legal right, it too has been pled. *See* CCAC ¶ 205 n.72 (discussing HIPAA authorization required before patient information shared); *see also* § V.A.1.

Plaintiffs' Benefit of the Bargain Damages Are Well Pled: In addition, Plaintiffs allege that Google's conduct violates the limited "data license" Plaintiffs provided to Google in exchange for the use of its services, and a host of governing laws, such that Plaintiffs "surrendered more" data—property—to Google than they intended or reasonably expected. CCAC ¶¶ 277-83, 377, 383-87.

4. Plaintiffs Have Established Irreparable Harm

As discussed above, Plaintiffs have submitted proof of past harm and they have alleged the risk of future injury sufficient to pursue injunctive relief. *See supra* § V.A.

Google argues that the requested relief is moot with respect to MedStar or Alton, which removed the Google Source Code only from the patient portals (MTD at 29), but this voluntary removal does not apply to the entire web property, or even begin to address Plaintiffs' motion to prohibit Google from using the Health Information *already collected* about these patients. *See* MPI at 1-3. Further, a claim becomes moot only when it is "absolutely clear that the allegedly wrongful behavior could not reasonably be expected to recur." *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs.*, 528 U.S. 167, 189 (2000). The assurance only applies to Medstar, not Google.

Google argues that harm is speculative because Plaintiffs have not proven Google can link data to them for targeted ads. *See* MTD at 29. The record demonstrates otherwise. *See* § III.B, C. Further, the law is clear that the invasion itself is a harm that warrants protections; subsequent linking is not required. *See In re Meta Pixel*, 2022 WL 17869218 at *17 (noting "[t]he invasion of privacy triggered by the Pixel's allegedly ongoing disclosure of plaintiff's medical information is precisely the kind of intangible injury that cannot be remedied by damages").

5. The Balance of Equities Favors an Injunction

Google argues it "would be excessively burdensome and/or infeasible" for Google to identify the full scope of its misconduct. *See* MTD at 30. *First*, "too-big-to-follow-the-law" is not a recognized defense to any claim. *Second*, identification is feasible (CCAC ¶¶ 178-95), and Plaintiffs set forth a tiered process to do so (MPI at 1-3). Google criticizes Plaintiffs' proposed process by claiming that verticals referenced in Plaintiffs' CCAC are "deprecated" and "entirely

separate from GA." MTD at 20 n.12. But this assertion is misleading (*see* Shafiq Reb. Decl. ¶¶ 57-62) and cleverly avoids addressing whether Google still uses verticals for any of the other products at issue, including Google Ads or Google Display Ads. In balancing the equities, Plaintiffs and class members should not bear the brunt of harm merely because Google's misconduct is so far reaching; particularly, where, as here, Plaintiffs have proposed a reasonable and feasible process.

6. An Injunction Is in the Public Interest

Google argues that other than privacy, there is "no basis for why a preliminary injunction would serve the public interest." MTD at 31. This is not a credible argument. The public interest is more than clear where Google Source Code on Health Care Provider properties impedes patient rights and ability to freely communicate with Health Care Providers; violates expectations of privacy, and breaches longstanding protections of health-related information and communications. That these privacy expectations and rights should be protected—indeed, that the laws should be upheld—is of the utmost interest to the public. And while Google strives to articulate a counterargument, the fact remains that any purported benefit to a web property is negligible when weighed against the public need to protect and enforce privacy rights relating to Health Information. Further, it is undisputed that Google Source Code is not necessary for the functionality of any Health Care Provider property. It can be, and has been, removed from Heath Care Provider web properties without any ill-effects on patients. The AHA Letter Google cites for this argument in fact agrees with Plaintiffs that adherence to privacy laws will "*enhance* provider-patient relationships by providing heightened privacy protections for information about care." MTD at 31; Dkt. 48-48. Nowhere in the letter does AHA advocate for Google's intrusive surveillance and collection of Health Information. Notably, Google itself has publicly stated that its source code, specifically GA, is inappropriate for Health Care Providers. *See* CCAC ¶ 8 *citing* Google, *HIPAA and Google Analytics*. The same would be true for the other at-issue products.

7. Plaintiffs' Injunctive Relief Is Defined with Particularity

Google argues the proposed relief is not sufficiently clear, but Google really complains about the scope of the relief, not its clarity. *See* MTD at 32 (arguing Google cannot identify all Health Care Providers at issue). Plaintiffs propose particular relief, reasonably clear and detailed

such that an ordinary person would know precisely what action is being proscribed. *See* MPI at 1-4. No more is required. *Portland Feminist Women's Health Ctr. v. Advocs. for Life, Inc.*, 859 F.2d 681, 685 (9th Cir. 1988); *E. & J. Gallo Winery v. Gallo Cattle Co.*, 967 F.2d 1280, 1297 (9th Cir. 1992) ("Injunctions are not set aside under Rule 65(d) unless they are so vague that they have no reasonably specific meaning"). Google's authority is inapposite. *See U.S. v. Holtzman*, 762 F.2d 720, 726 (9th Cir. 1985) (resolving inconsistency between two paragraphs of injunction); *Lamont v. Krane*, 2019 WL 2010705, at *4 (N.D. Cal. May 7, 2019) (plaintiff inadequately explained "types of harm" and thus did not establish the threshold "immediate threatened injury").

8. Provisional Class Certification Should Be Granted

Plaintiffs meet Rule 23(b)(2)'s requirements to pursue injunctive relief on behalf of the Class, which consists of similarly situated Internet users who, like Plaintiffs, have not consented to, have been, and are being harmed by Google's collection and use of their Health Information.

Google argues that class certification is not necessary because Plaintiffs "do not plan to use" the enumerated properties again. *See* MTD at 32. Plaintiffs allege they would like to use the properties; they should be able to use them; and they cannot because Google is present there surveilling what should be protected communications. Plaintiffs' pursuit of their—and class members'—ability to use this important mode of communication with Health Care Providers free from Google's interference is a reason to *grant* Plaintiffs' motion, and quickly, not to deny certification. Google also argues that the injunction would "have the effect of prohibiting the use of GA" for class members. Yet Google concedes that consumers do not "use" Analytics. *See* MTD at 33, n.14. No harm will come to class members if Plaintiffs' motion is granted. Moreover, an order prohibiting Google from using the collected data, also a subject of this motion, would benefit any putative Class member whether or not they visit the same website again.

Google also challenges commonality under Rule 23(a), but that is satisfied by even a *single* common question. *See* MTD at 33-34; *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 350 (2011). Multiple common questions, and common answers, are raised here. *See* CCAC ¶ 306. Google's remaining arguments do not undermine the commonality of the issues presented:

Consent: The relevant consent issues here involve analysis of federal law, expectations of

privacy for health information and communications, and Google's public statements—each of which is identical for all class members and assessed from an objective, reasonable person standard. Google cannot rely on Health Care Providers' statements to establish consent. *See Brown*, 2023 WL 5029899, at *13 ("Courts apply the reasonable person standard to determine consent") (quotation omitted); § V.A.2.

Communications: Plaintiffs' requested relief is tailored to conduct that violates the law. Google's communications argument ignores unrebutted evidence showing Google activity throughout the properties identified in the Smith Declaration, and Plaintiffs' proposed relief sets up a discovery process to determine the scope with respect to other properties. To the extent a given Health Care Provider used Google Source Code in a mixed fashion—i.e., some legal and illegal activity—the onus should be on Google (the wrongdoer) to resolve these issues. *See Westinghouse Elec. & Mfg. Co. v. Wagner Elec. & Mfg. Co.*, 225 U.S. 604, 621 (1912) ("[a]ll the inconveniences of the confusion [between legal and illegal property] is thrown upon the party who produces it, and it is for him to distinguish his own property or to lose it"); *U.S. v. Fed. Mail Ord. Corp.*, 47 F.2d 164, 165 (2d Cir. 1931) (Hand, J.) ("if the smuggler can effectively block [enforcement] by mingling the smuggled goods into a mass of fungibles, from which no one but him can separate them," then it is "reasonable to take the whole and leave it to him who confused them to disentangle the innocent from the guilty"); *Micro Lithography Inc. v. Inko Indus. Inc.*, 1991 WL 332053, at *6 (Cal. App. 1991) (burden on defendant "to show what portion of its profits is not attributable" to the wrongful conduct – not plaintiff or the Court).

Use of GA by Websites: Minor variations in how websites use Google Source Code (which is not only GA as Google suggests) do not defeat commonality where they all use it and all send Health Information to Google.

Choice of Law: Google's choice of law and extraterritoriality arguments are also unavailing. Plaintiffs' MPI does not require application of the law of multiple jurisdictions or the extraterritorial application of California law. The motion is predicated on the ECPA, CIPA, common law intrusion, and the UCL. The ECPA is a federal statute that applies to all class members. Likewise, CIPA, intrusion upon seclusion, and the UCL, based on California law, will

apply to all class members because Google's terms of service adopts California law, Google is headquartered in California, and the misconduct emanated from Google's decision-making processes in California. *See* CCAC ¶ 12; *Maldonado v. Apple, Inc.*, 2021 WL 1947512 (N.D. Cal. Apr. 21, 2021) ("the named plaintiffs represent a class in which one state's law applies – the law selected via contract"); *Schmitt v. SN Serv. Corp.*, 2021 WL 3493754, at *3 (N.D. Cal. Aug. 9, 2021) (and cited cases) (no extraterritorial application of California law where the defendant was headquartered, and the alleged misconduct occurred, in California); *Wang v. OCZ Tech. Grp., Inc.*, 276 F.R.D. 618 (N.D. Cal. 2011). Finally, Google offers no explanation as to why Health Care Providers' terms of services would apply to Plaintiffs' claims against *Google* for *Google's* misconduct. The Court should provisionally certify the Class.

B. MOTION TO DISMISS

To state a claim, a plaintiff need only allege sufficient facts to "allow[] the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 663, 678 (2009); *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "Heightened fact pleading of specifics" is not required. *Twombly*, 550 U.S. at 555, 570. Further, the Court "accepts all factual allegations as true and draws all reasonable inferences in favor of the plaintiff." *Usher v. City of Los Angeles*, 828 F.2d 556, 561 (9th Cir. 1987).

1. Heightened Standard of Rule 9(b)

Plaintiffs' claims under the ECPA, CIPA, UCL, Contract Claims, and Unjust Enrichment (Counts 1, 2, 5, 10-13 and 14) do not sound in fraud and thus are not subject to Rule 9(b). To the extent the Court disagrees, and views any remaining claim as sounding in fraud, Plaintiffs have easily met Rule 9(b)'s requirement. Plaintiffs allege that Google (who, CCAC ¶ 32), unlawfully tracked, re-directed, collected and used patients' Health Information (what, ¶¶ 37-43, 102-12, 119-22, 135, 143-44, 161, 168) through the use of the Google Source Code (how, ¶¶ 39-42, 171, 175) on Health Care Provider web properties (where, ¶¶ 51-64), and that this occurred in real time, as patients were communicating with their Health Care Provider (when, ¶¶ 53-57). *See Klein v. Facebook, Inc.*, 580 F. Supp. 3d 743, 795 (N.D. Cal. 2022).

2. Plaintiffs Adequately Pled Trespass to Chattels

The theory of Plaintiffs' trespass cause of action is that Google intentionally took "actions to lodge Google Cookies on [Plaintiffs'] computing devices," resulting in Google's ever-present and unavoidable surveillance on the devices, reducing storage space, and fundamentally impairing the devices' value and functioning for ordinary, intended operations. *See* CCAC ¶¶ 19-31, 333, 385, 396-403. Stated another way, the inevitability that Google's Cookies will be lodged on Plaintiffs' devices upon visiting a Health Care Provider web property leaves Plaintiffs only two choices: submit to Google's intrusion into their healthcare communications in violation of reasonable expectations of dignity, privacy, and justice (*id.* ¶¶ 18, 196-250, 333, 387, 401-03), or do not use their compromised devices for a purpose for which they wish to use them, and should be able to use them. Google makes three arguments for dismissing this claim, but none has merit.

Intent: Plaintiffs adequately plead intent, including allegations that Google's actions, from creating the Google Source Code and providing it to Health Care Providers (*e.g.,* CCAC ¶¶ 4-6, 40-41, 44, 48-50, 71), to misleading the Class (*id.* ¶¶ 243-50) were intended to cause Google Source Code to interfere with their devices. *See* Rest. 2d Torts § 217(c) ("Intention is present when an act is done for the purpose of . . . or with knowledge that [] intermeddling will, to a substantial certainty, result from the act"); *id.* § 217(d) ("indirect result of an act" supports liability); *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1351 (2003).

Interference with Personal Property: Plaintiffs' theory defends property interests in their computing devices, not data. *See* MTD at 37. Thus, Google's cases about "property" are inapposite.

Adequate Harm: To plead trespass harm to a computing device, Plaintiffs need only allege Google impaired the condition, quality, or value to Plaintiffs of their personal property, or interfered with Plaintiffs' use of personal property. *Grace v. Apple Inc.*, 2017 WL 3232464, at *5, *11-13 (N.D. Cal. July 28, 2017). Alleging "physical" interference is not required, although Plaintiffs also allege a loss of storage space. *See* CCAC ¶ 404; Rest. 2d Torts § 218(h) (discussing actionable non-physical injuries: "[T]he use of a toothbrush by someone else may lead a person of ordinary sensibilities to regard the article as utterly incapable of further use by him, and the

wearing of an intimate article of clothing may reasonably destroy its value in his eyes"). While the inability to conduct some activities on Plaintiffs' devices is not complete diminution of value, it need not be to state a claim. *Cf. Grace*, 2017 WL 3232464, at *11-13 (injury alleged where Apple disabled ability to FaceTime, one of devices' intended functions); *Soo v. Lorex Corp.*, 2020 WL 5408117, at *9 (N.D. Cal. Sept. 9, 2020) (same, defendant diminished functionality of camera and offered inadequate replacement); *San Miguel v. HP Inc.*, 317 F. Supp. 3d 1075, 1088 (N.D. Cal. 2018) (same, defendant prevented use of certain ink cartridges with printers).

Google's authority is not on point. *Casillas v. Berkshire Hathaway Homestate Ins. Co.*, 79 Cal. App. 5th 755, 765, 768 (2022), involved a one-time copying of files where no allegation of impairment or loss of use was even made. Similarly, *WhatsApp Inc. v. NSO Grp. Techs. Ltd.* involved impairment of "services," but no allegation that the relevant devices lost value or became unusable in any way. 472 F. Supp. 3d 649, 685–86 (N.D. Cal. 2020). In *LaCourt v. Specific Media, Inc.*, plaintiffs "all but abandoned" any theory that cookies compromised devices' performance or value. 2011 WL 1661532, at *5, 7 (C.D. Cal. Apr. 28, 2011). Similarly, in *Kurowski v. Rush Sys. for Health*, the court found "physical disruption" was not alleged, and distinguished plaintiff's authority concerning pop-up advertisements that physically impaired the use of devices. 2023 WL 4707184, at *9–10 (N.D. Ill. Mar. 2, 2023). Notably, *Kurowski* did not hold that actionable harm *cannot* be pled if defendant's conduct was "invisible and surreptitious," as Google argues, but rather that unobtrusive intrusions were inconsistent with the authority presented there. *See id.*; MTD at 38. By contrast, Plaintiffs here allege, support, and explain why their devices have lost value to them consistent with the Restatement and this District's case law. *See* CCAC ¶¶ 401-04. Plaintiffs' plausible allegations suffice at this stage. *See Craigslist Inc. v. 3Taps Inc.*, 942 F. Supp. 2d 962, 981 (N.D. Cal. 2013).

3. Plaintiffs Adequately Pled Statutory Larceny

California Penal Code § 496 authorizes civil actions against persons who receive property "obtained in any manner constituting theft." "Theft" includes a simple nonconsensual taking and theft by false pretense, which is "the consensual but fraudulent acquisition of property from its owner." Cal. Penal Code § 484(a); *Bell v. Feibush*, 212 Cal. App. 4th 1041, 1049 (2013). Plaintiffs

may plead theories of theft in the alternative. *See* Cal. Crim. Jury Instruction No. 1800.

Consistent with the above, Plaintiffs allege that Google obtained their Health Information unlawfully (CCAC ¶¶ 1, 8-9, 408-17), and Google's arguments to the contrary are without merit.

Simple Theft: Google erroneously argues that data generated from websites is not property owned or possessed by Plaintiffs. Judge Koh rejected this argument in *Calhoun.* In doing so, Judge Koh relied, in part, on the Ninth Circuit's decision in *FB Tracking,* and concluded that "California courts have [] acknowledged that users have a property interest in their personal information." *Calhoun*, 526 F. Supp. 3d at 635 (citations omitted). As noted above, *Calhoun* dealt with much of the same information that is at issue here. *See id.* at 613; CCAC ¶¶ 33-36; *supra* § V.A.3.d. Google strains to distinguish *Calhoun*, but Judge Koh's analysis is on all fours and faithfully applied the Ninth Circuit's guidance that "property" law *does* protect consumers' property rights in their data.

Further, Google asserts that Plaintiffs must "establish a tort of trespass." MTD at 29 *citing People v. Brock*, 143 Cal. App. 4th 1266 (2006). But Google's own authority clarifies that the "trespass" inquiry asks the same questions as *Calhoun*: "The act of taking personal property from the possession of another is always a trespass *unless the owner consents* to the taking freely and unconditionally or the taker has a legal right . . . ." 143 Cal. App. 4th at 1275. Plaintiffs plausibly allege that they did not consent and that Google nonetheless took their property (CCAC ¶ 412), just as plaintiffs did in *Calhoun*. Plaintiffs also plead "asportation," which merely requires "defendant moved the property, even a small distance, and kept it for any period of time." Cal. Crim. Jury Instruction No. 1800; CCAC ¶¶ 48-50 (discussing "data flow" to Google).

Theft by False Pretenses: Google's focus on the common law requirement of "title" transfer is a red herring. Plaintiffs need not allege transfer of title to state a claim. California enacted a larceny *statute* precisely because "it was difficult at times to determine whether a defendant had acquired title" to distinguish "false pretenses" from other forms of theft. *People v. Williams*, 57 Cal. 4th 776, 785 (2013) ("Juries need no longer be concerned with the technical differences between the several types of theft, and can return a general verdict of guilty if they find [] an 'unlawful taking.'"). Nor are Plaintiffs required to allege that their unlawfully taken property was "tangible." Google's resort to unpublished decisions that do not even discuss intangible property

speaks volumes about the merits of its argument. *See* MTD at 39.

4. Plaintiffs Adequately Pled CDAFA Violations

"The CDAFA is California's computer abuse law." *Oracle USA, Inc. v. Rimini St., Inc.*, 879 F.3d 948, 960 *rev'd in part on other grounds* 139 S. Ct. 873 (2019). A fundamental purpose of the CDAFA is to "expand the degree of protection afforded to individuals" from "interference, damage, and unauthorized access to lawfully created computer data and [] systems," because such protections are "vital to the protection of [individuals'] privacy." Cal. Penal Code § 502. Plaintiffs adequately plead their claims under CDAFA §§ 502(c)(1-3) and (6-8).

a) Plaintiffs Have Standing Under Penal Code § 502(e)(1)

Section 502(e)(1) of the CDAFA authorizes "[t]he owner or lessee of the computer, [system, network, or program], or data who suffers damage or loss by reason of a violation" to bring a civil suit for compensatory damages and equitable relief. "[A]ny amount of damage or loss caused by the defendant's CDAFA violation is enough to sustain the plaintiff's claims." *NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 954, 964 (N.D. Cal. 2014). Nonetheless, Google disputes all five categories of damage or loss alleged. *See* MTD at 40-43. Each theory (CCAC ¶¶ 437-38) supports Plaintiffs' CDAFA standing, for the following reasons:

Interruption and preclusion of communications with Health Care Providers, and inability to use devices for that purpose, are plausibly alleged. Google's challenge based on *Kurowski*, where no CDAFA claim was even asserted, fails for the reasons discussed above (*supra* § V.B.2). "Surreptitious" conduct is consistent with CDAFA liability. *Cf. In re Carrier IQ, Inc.*, 78 F. Supp. 3d at 1101 (allegation of "deeply hidden" conduct supported CDAFA claim).

Damaged relationships with Health Care Providers are plausibly alleged because Google deprived doctors and patients of an important, convenient way to communicate, and involved Providers in violating medical privacy. At minimum, this damage can be inferred. *See Usher*, 828 F.2d at 561; *Lindsay-Stern v. Garamszegi*, 2016 WL 11745948, at *6 (C.D. Cal. Oct. 13, 2016).

Recoverable expenditures are plausibly alleged. Plaintiffs cannot control Google or Healthcare Providers, so responding to Google's CDAFA violations required Plaintiffs to change how, and whether, they use computing devices on Health Care Provider websites, and to retain

counsel to pursue the only other means available to stop Google's CDAFA violations—an injunction. *See* CCAC ¶¶ 333, 380, 385, 388. Both responses required investigating the problem and the perpetrator(s), among other work. *See Facebook, Inc. v. Power Ventures, Inc.*, 2010 WL 3291750, at *4 (N.D. Cal. July 20, 2010) (standing established where plaintiff "expended resources," even if only a few "clicks of a mouse" and some "keystrokes"). Google's argument that § 502(e)(1) *limits* compensatory damages (the statute says damages shall *include* certain costs) is specious. *See e.g.*, *Mintz v. Mark Bartelstein & Assocs. Inc.*, 906 F. Supp. 2d 1017, 1032 (C.D. Cal. 2012) (time investigating violator's identity compensable). Attorneys' fees are not redundant—they compensate *counsel's* work, not Plaintiffs'. Cal. Penal Code § 502(e)(2).

Diminution in value is a valid theory of damage or loss and plausible here. *See FB Tracking*, 956 F.3d at 600 (reversing dismissal of CDAFA claim, finding requisite damages based on allegations of data's value and "legal interest in unjustly earned profits" from defendant's use of it); *Brown*, 2023 WL 5029899, at *19 (N.D. Cal. Aug. 7, 2023) (after *FB Tracking*, "plaintiffs can state an economic injury [under the CDAFA] for their misappropriated data"). Google's Third Circuit authority predates *FB Tracking*, and Plaintiffs' factual allegations regarding a market for their data, and Google's unjust enrichment through their misappropriated data, distinguish *Cottle*, 536 F. Supp. 3d at 484 and *Wesch v. Yodlee, Inc.*, 2021 WL 6206644 (N.D. Cal. July 19, 2021). *See* CCAC ¶¶ 267-93, 440.

b) Plaintiffs Own Their Health Information

Google's reference to "event level data" misconstrues Plaintiffs' claim, which is based on their ownership of their Health Information, not the "event level data" through which Google collects the Information. *See Lindsay-Stern*, 2016 WL 11745948 at *5-6 (an "ownership *interest*" in data subject to a CDAFA violation is sufficient to plead "damage or loss") (emphasis added). Moreover, fact questions about who "generate[s]" the data cannot be resolved on the pleadings. *Cf. Brown*, 2023 WL 5029899 at *19 (denying summary judgment on "evidence showing that Google receives data from users' browsers directly, not indirectly through third-party websites").

Further, Google cites to *Alderson v. U.S.*, where plaintiffs unsuccessfully asserted property rights in knowledge of their employer's wrongdoings, which formed the basis of a *qui tam* claim.

718 F. Supp. 2d 1186 (C.D. Cal. May 27, 2010). *Alderson* did not involve the plaintiffs' personal information, and it merely stands for the proposition that property rights require a "legitimate claim to the exclusive possession of that right and is capable of excluding others from such possession." 718 F. Supp. 2d 1186, 1197 (C.D. Cal. May 27, 2010). Plaintiffs' Health Information meets this standard. *See* CCAC ¶¶ 295 (citing cases recognizing property rights in personal information); 296 (federal and state law grant patients right to protect confidentiality of their Health Information); 297 (citing cases recognizing property rights in communication contents). Google's unlawful collection and use of Plaintiffs' Health Information does not make Plaintiffs' property rights any less legitimate.

c) Plaintiffs Allege the Requisite Scienter

Plaintiffs allege that Google took specified actions "knowingly" *and* "without permission," as required to state claims under § 502(c)(1-3), (6-7). Cal. Civ. Jury Instruction No. 1812; CCAC ¶¶ 430-31, 435. Google contends that Plaintiffs must also plead "Google knew it acted without permission," relying on a principle of statutory interpretation. Google is incorrect. The Ninth Circuit has "explicitly rejected the notion" Google advances here, explaining that the principle is "specific to particular grammatical contexts" that are not presented by the CDAFA. *U.S. v. Price*, 980 F.3d 1211, 1220-21 (9th Cir. 2019).

5. Plaintiffs Adequately Pled Aiding and Abetting

Aiding and abetting occurs where a defendant either "'(a) knows the other's conduct constitutes a breach of duty and gives substantial assistance or encouragement to the other to so act or (b) gives substantial assistance to the other in accomplishing a tortious result and the person's own conduct, separately considered, constitutes a breach of duty.'" *Casey v. U.S. Bank Nat. Assn.*, 127 Cal. App. 4th 1138, 1144 (2005).

Here, Health Care Providers owe Plaintiffs and class members a duty arising from the California Constitution (CCAC ¶ 450), their receipt of health data, and their status as fiduciaries (*id.* at ¶¶ 443-45). *See e.g.*, *Stasi v. Inmediata Health Grp. Corp.*, 501 F. Supp. 3d 898, 914 (S.D. Cal. 2020) (recognizing "common law duty" of "companies that possess personal and medical information") (collecting cases); *Hahn v. Mirda*, 147 Cal. App. 4th 740, 748, (2007) ("The doctor-

patient relationship is a fiduciary one"). Plaintiffs plausibly allege that Google knew of their breach of duty because the Health Information wrongfully disseminated went to *Google*, which used it for advertising and other purposes. *See* CCAC ¶¶ 6, 32, 111, 414; *see also Opperman v. Path, Inc.*, 84 F. Supp. 3d 962, 986 (N.D. Cal. 2015) (inferring knowledge of data collection from Apple's "development of APIs that permitted Apps to access" data and extent to which Apple was "involved in and controlled the development and functions of Apps").

Separately, as explained herein, Google owed a duty to Plaintiffs and class members arising from its own promises, the California Constitution, and as a possessor of Health Information. *Stasi,* 501 F. Supp. 3d at 914. It knew that its role in facilitating the dissemination of Healthcare Information would lead to a tortious result because the disclosure and use of health data is an obvious invasion of privacy. *In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1143 (C.D. Cal. 2021). Google provided "substantial assistance" to Health Care Providers because it provided the Source Code that was used to accomplish this tortious result and breach of duties. *See* CCAC ¶¶ 453-54; *see also* Shafiq Reb. Decl. ¶¶ 8-19. Google disputes the allegations of substantial assistance, but they are factually supported and all the more plausible because Google stood to profit from the misappropriated Health information. *See Ray v. BlueHippo Funding, LLC*, 2008 WL 1995113, at *4 (N.D. Cal. May 6, 2008) (liability appropriate where computer company "sought to profit from what it allegedly knew were unlawful practices"); *In re First All. Mortg. Co.*, 471 F. 3d 977, 999 (9th Cir. 2006); *Schulz v. Neovi Data Corp.*, 152 Cal. App. 4th 86, 96 (2007). Plaintiffs therefore allege more than mere "aware[ness]" of wrongdoing, or some unrelated relationship between Google and Health Care Providers, distinguishing the two cases Google relies on. *See* MTD at 44 *citing Chetal v. Am. Home Mortg.*, 2009 WL 2612312, at *4 (N.D. Cal. Aug. 24, 2009); *Decarlo v. Costco Wholesale Corp.*, 2020 WL 1332539, at *5–6 (S.D. Cal. Mar. 23, 2020).

Plaintiffs' allegations are not "conclusory." *See supra* § III.A.2-.3. Unlike in *Cousin v. Healthcare*, 2023 WL 4484441, at *3 (S.D. Cal. 2023) and *Kurowski*, 2023 WL 4707184 at *3, Plaintiffs sufficiently allege what information Google obtained. Google's consent defense premised on Kaiser's privacy policy is illogical. *See* MTD at 44 *citing* Dkt. 49-26 ("explaining

Kaiser "may" use "cookies" that are a "unique identifier *that does not contain information about your health history*"); *see also supra* §§ III.A.2, V.A.3.c.

Lastly, Google's contention that California law cannot apply (MTD at 44) contradicts the facts alleged (*supra* § V.A.8), and is also "premature." *See Fitzhenry-Russell v. Coca-Cola Co.*, 2017 WL 4680073, at *4 (N.D. Cal. Oct. 18, 2017). That some of Plaintiffs' counsel in a separate case brought claims where a different defendant is headquartered is an unremarkable fact that says nothing about what law applies to Google. *See* MTD at 44 *citing Cousin*, 2023 WL 4484441.

6. Plaintiffs Adequately Pled Breach of Contract

Plaintiffs' claims based on Google's breach of its Terms of Service ("TOS") and Privacy Policy are well-pled. At the threshold (MTD at 45), Google disputes that it has a relevant contract, but the first sentence in the body of Google's TOS tells users that it "reflect[s] the way Google's business works" for anyone "using [its] services." Dkt. 49-13 at 2. Google's Privacy Policy, which the TOS incorporates (*id.*), also fails to differentiate among "services" and expressly states that it covers "[p]roducts that are integrated into third-party apps and sites, like ads, analytics, and embedded Google Maps" (Dkt. 49-20 at 2). When Plaintiffs visit Health Care Provider web properties that contain Google Source Code, they are interacting with Google services. Google's contract does not state anywhere that its promises are non-binding when consumers interact with Google's services on non-Google websites. Google's promises are unequivocal; Plaintiffs have not "altered" the text of the TOS, as Google asserts, and to the extent Google's commitments are unclear, ambiguities should be resolved against Google, "the draftsman." *Daniel v. Ford Motor Co.*, 806 F.3d 1217, 1224 (9th Cir. 2015); *see also* Cal. Civ. Code § 1654.

Plaintiffs need only allege one breach to state a claim. They adequately plead eleven (and withdraw the claim based on Breach 7).

Breach 1: As Google Account Holders, Plaintiffs agreed to Google's TOS in exchange for Google's promise that other Google users like Health Care Providers "*must* follow [] basic rules of conduct" such as complying with laws, respecting privacy, and refraining from misleading or fraudulent conduct. Dkt. 49-13 at 5 (emphasis added). Google's argument that the TOS contains *users'* promises to *Google*, not vice versa, conflicts with its own characterization of the contract:

"These Terms [] [] reflect the way Google's business works, the laws that *apply to our company*," and "define *Google's relationship with you* as you interact with our services." *Id.* at 1 (emphasis added). Further, if Google's TOS only imposed obligations on users—and not Google—the entire contract would fail for lack of mutuality. *See Lantis Laser, Inc. v. Ice Cold Stocks, LLC*, 2008 WL 11338191, at *2 (C.D. Cal. Sept. 23, 2008). Instead, Google undertook a contractual duty to impose an enforceable code of conduct amongst Google users. Google's argument that it cannot make good on its promise is not grounds for dismissal but, instead, evidence of its breach.

Breach 2: Plaintiffs allege Google breached its promise that it collects "[h]ealth information *if you choose to provide it*[.]" CCAC ¶ 475 (emphasis added); Dkt. 49-20 at 18. This statement—*if you choose*—creates the reasonable expectation of an "opt-in" environment. That is, users have an *affirmative choice* to opt-in to letting Google track and collect their "health information." By giving users no actual choice in this respect, Google breaches this promise.

Google's quibble over its definition of "health information" is unavailing. Google's Privacy Policy describes "health information" as "your medical history, vital signs and health metrics (like blood glucose levels), *and other similar information related to your physical or mental health*[.]" *Id.* Plaintiffs allege Google breached this promise by collecting information about Plaintiffs' patient status, doctors, conditions, treatments, requests for appointments, and prescriptions (CCAC ¶¶ 2, 33-36, 476)—all of which constitute "information related to [Plaintiffs'] physical or mental health" and "medical history" when Plaintiffs did *not* choose to provide it to Google. Google's argument that the Privacy Policy does not mean what it says but, instead, means "actual medical information" as defined by Google, but not "pseudonymous" information, and not "web activity data from which assumptions may be made about a person" asks the court to resolve fact disputes, draw inferences, and interpret contract terms in Google's favor. *See* MTD at 46. That would be improper on this motion. *See Hall v. FCA US LLC*, 2022 WL 1714291, at *1 (9th Cir. May 27, 2022) (and cited cases). Google's authority, *Smith v. Facebook, Inc.*, does not hold otherwise. In *Smith*, there were no ambiguities or fact disputes to resolve. 262 F. Supp. 3d 943, 954 (N.D. Cal. May 9, 2017). Further, the putative class was not limited to patients; the healthcare websites were not limited to covered entities; and the Facebook

contract at issue did not have any promises relating to "Health Information" as alleged here. *See generally id.*

Google also points to a portion of its Privacy Policy that states Google collects web and app activity, which can be altered by certain user settings, asserting that Plaintiffs must have disabled these settings to state a claim for Breach 2. *See* MTD at 46. Even if the controls could have stopped Google, which Plaintiffs dispute, Google ignores a cardinal rule of contract interpretation: specific terms control over general ones. *S. Cal. Gas Co. v. City of Santa Ana*, 336 F.3d 885, 891 (9th Cir. 2003). Google *specifically* promised that it will only collect "health information" if Plaintiffs "choose to provide it." Therefore, Plaintiffs do not have a contractual obligation to implement additional "controls" to prevent Google from doing what it promised not to do. Google's cited case is inapposite. *See Google Asst.*, 457 F. Supp. 3d at 830 (dismissing contract claim where contract specified "personal information" *would* be shared in three circumstances and plaintiffs failed to plead circumstances were inapplicable).

Breaches 3-6: Google makes several promises that it does not show personalized advertisements based on health and prohibits advertisers from utilizing health information for personalized advertising. CCAC ¶¶ 477-80. Plaintiffs allege (and support with the Smith Decl. and the Shafiq Reb. Decl.) that Google breached these promises by utilizing Health Information for targeting advertisements and by failing to disable remarketing lists that do not comply with Google's personalized advertising policy. *See* CCAC ¶ 481; *see also* § III.B. Google's arguments that its advertisements are not "personalized" or based on "users" data (MTD at 47) dispute the facts alleged, at most raising questions to resolve on the merits, not here. Google's argument about whether Plaintiffs *viewed* the offending advertisements raises fact questions that are not even relevant to this breach, which concerns Google's *use* of Plaintiffs' Health Information in violation of its express promises; not which ads Google showed as a result. "[A] breach of contract claim accrues at the moment of breach and the injury, for standing purposes, is the breach itself." *In re Google Referrer Header Priv. Litig.*, 465 F. Supp. 3d 999, 1010 (N.D. Cal. 2020).

Breaches 5, 6, 8-12: Google made a number of promises to users via documents that Google incorporates into its Privacy Policy via hyperlinks. *See* CCAC ¶ 472. Google disputes that it

incorporated these documents by reference (MTD at 47-48), but "California case law makes it quite easy to incorporate a document by reference." *FB Cons. Priv.*, 402 F. Supp. 3d at 791. "What's needed is simply that the reference to the document be unequivocal, that the document be called to the attention of the contracting parties, and that the terms of the document be easily available to the contracting parties." *Id.*

Google does not dispute that it called these documents to Plaintiffs' attention and made them readily available from the Privacy Policy. Google argues that it did not "reference" each document, by name. *See* MTD at 47-48. California law is not so arbitrary. References to the *documents* that form the bases of these claims are unequivocal, substantive, and clear. While Google may not have always specified the "title" of each Help Page in the text presented, it identified the subject matter of each hyperlink (sometimes mirroring the "title"), providing details that are *more* descriptive than the title. *See* CCAC ¶ 472; Dkt. 49-20 (hyperlinks underlined), at 31 ("We don't use topics or show personalized ads based on…health. And we require the same from advertisers that use our services," linking to Dkt. 49-17, entitled "Personalized advertising," containing Promise 5); *see also* Dkt. 49-20 at 34 ("Learn more about how Google uses data when you use our partners' sites or apps," linking to untitled page with heading "How Google uses Information from Sites of Apps that Use our Services," containing Promise 8); *id.* at 10 (again incorporating specified document, *with* heading). *See* Dkt. 49-20 at 29 ("an advertiser may want to use its Google Analytics data to create more relevant ads…Learn more") (linking to page titled "Safeguarding your data" containing Promise 9). These linked documents similarly incorporate other documents related to Promises 6 and 10-12. The "require the same from" hyperlink at issue in Breach 5 links to Dkt. 49-17, which states "Legal restrictions: Ads must comply with the law," which hyperlinks Dkt. 49-18 entitled "Healthcare and Medicine", stating "Learn about what happens if you violate our policies," containing Promises 6, 10, 11. The "require the same from" hyperlink at issue in Breach 5 also links to "Legal Requirements" which contains Promise 12.[6] Google's informative, substantive, and unequivocal references to the documents, their subject

[6] Google changed Promise 12 *after* Plaintiffs filed their CCAC. *See* Barnes Suppl. Decl. ¶¶ 22-24.

matter, and in some cases their titles, distinguishes Plaintiffs' claim from the hyperlink that only said "Learn More" in Google's sole cited authority. *See Rodriguez v. Google LLC*, 2021 WL 6621070, at *4 & n.4 (N.D. Cal. Aug. 18, 2021).

7. Plaintiffs Adequately Pled Breach of Implied Contract

Plaintiffs' implied contract claims are based on Google's conduct and the surrounding circumstances such as Google's various promises that it will not track, collect, or use Plaintiffs' Health Information, legal protections regarding Health Information (*i.e.*, federal, state, and common law protections), and Plaintiffs' reasonable expectations of privacy. *See* CCAC ¶¶ 500-01, 519-20. These allegations are sufficient to establish mutual agreement and intent.

Google is wrong in contending that implied contract claims are improperly duplicative here. Count 11 is expressly alleged in the alternative and "[t]o the extent the Google Terms of Service and Privacy Policy are not express contracts" (CCAC ¶ 496), and Count 12 is brought on behalf of a subclass of individuals who do not have Google accounts (*id.* ¶ 514).

Google is wrong about non-account holders. As to Count 12, Google states in its Privacy Policy that no Google Account is required to use the services, and the terms apply regardless. Dkt. 48-20 at 2; CCAC ¶ 515. These factual allegations answer Google's questions about whether it made any promises to them, and there can be little doubt that Google will argue, when it suits Google, that non-users should be held to have read and be bound by those terms.

Finally, Google inaccurately argues that Plaintiffs' expectations of privacy are subjective and "unilateral." Not so. Plaintiffs' alleged expectations are objectively reasonable. *See* CCAC, ¶¶ 196-266; § V.A.3.c; *Meta Pixel*, 2022 WL 17869218 at *15; *FB Tracking.*, 956 F.3d at 605-06.

8. Plaintiffs Adequately Pled Breach of Implied Covenant of Good Faith and Fair Dealing

This claim is well pled because, contrary to Google's characterization (MTD at 50), Plaintiffs allege that Google "abused its power" to define key terms within the contract that are relevant to the collection and use of their Health Information. *See* CCAC ¶¶ 535-36. Google's overstepping the reasonable and intended boundaries of the contract frustrated Plaintiffs' rights to contractual benefits—which included being able to understand what information Google collects

and what Google does with it. *Id.* ¶¶ 535-38. Such misconduct is an actionable breach of the implied covenant of good faith and fair dealing because, as this Court has noted: "[i]n addition to explicit promises, every contract includes an implicit promise not to take an action that would deprive the other contracting party of the benefits of their agreement." *FB Cons. Priv.*, 402 F. Supp. at 802. Plaintiffs need not allege a breach of a specific provision, or that the "party's conduct be dishonest." *Carma Devs. (Cal.), Inc. v. Marathon Dev. Cal., Inc.*, 2 Cal. 4th 342, 372 (1992). "Objectively unreasonable conduct," evading "the spirit of the bargain," and "abuse of a power to specify terms," as adequately pled here, are all actionable. *Id.*; *see also R.J. Kuhl Corp. v. Sullivan*, 13 Cal. App. 4th 1589, 1602 (1993).

9. Plaintiffs Adequately Pled Unjust Enrichment

Plaintiffs allege that Google was unjustly enriched by their Health Information (CCAC ¶¶ 541-44) and lack an adequate remedy at law (*id.* ¶ 18). They are entitled to pursue an equitable remedy. *FB Tracking*, 956 F.3d at 600 ("California law requires disgorgement of unjustly earned profits"). Google takes issue with how plaintiffs identify the cause of action, but whether this Court treats unjust enrichment as a standalone claim or quasi-contract claim is beside the point. The claim is viable; it is distinct from the breach of contract claim (which alleges Google's failure to make good on its promises, *supra* § V.B.6), and Plaintiffs are permitted to pursue multiple theories even if they are "duplicative [] or superfluous." *Astiana v. Hain Celestial Grp., Inc.*, 783 F.3d 753, 762 (9th Cir. 2015).

VI. CONCLUSION

Plaintiffs respectfully request that the Court grant the Motion for Preliminary Injunction and deny Google's Motion to Dismiss.

Dated: August 24, 2023

SIMMONS HANLY CONROY LLC

/s/ Jason Barnes

Jason 'Jay' Barnes (admitted *pro hac vice*)
jaybarnes@simmonsfirm.com
Eric Johnson (admitted *pro hac vice*)
ejohnson@simmonsfirm.com
An Truong (admitted *pro hac vice*)
atruong@simmonsfirm.com
112 Madison Avenue, 7th Floor

New York, NY 10016
Tel.: 212-784-6400
Fax: 212-213-5949

LOWEY DANNENBERG, P.C.
Christian Levis (admitted *pro hac vice*)
clevis@lowey.com
Amanda Fiorilla (admitted *pro hac vice*)
afiorilla@lowey.com
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel.: (914) 997-0500
Fax: (914) 997-0035

KIESEL LAW LLP
Jeffrey A. Koncius, State Bar No. 189803
koncius@kiesel.law
Nicole Ramirez, State Bar No. 279017
ramirez@kiesel.law
Mahnam Ghorbani, State Bar No. 345360
ghorbani@kiesel.law
8648 Wilshire Boulevard
Beverly Hills, CA 90211-2910
Tel.: 310-854-4444
Fax: 310-854-0812

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
Michael W. Sobol, State Bar No. 194857
msobol@lchb.com
Melissa Gardner, State Bar No. 289096
mgardner@lchb.com
Jallé H. Dafa, State Bar No. 290637
jdafa@lchb.com
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Tel.: 415 956-1000
Fax: 415-956-1008

Douglas Cuthbertson (admitted *pro hac vice*)
dcuthbertson@lchb.com
250 Hudson Street, 8th Floor
New York, NY 10013
Tel.: 212 355-9500
Fax: 212-355-9592

SCOTT+SCOTT ATTORNEYS AT LAW LLP
Hal D. Cunningham, State Bar No. 243048
hcunningham@scott-scott.com

Sean Russell, State Bar No. 308962
srussell@scott-scott.com
600 W. Broadway, Suite 3300
San Diego, CA 92101
Tel.: (619) 233-4565
Fax: (619) 233-0508

Joseph P. Guglielmo (admitted *pro hac vice*)
jguglielmo@scott-scott.com
Ethan Binder (admitted *pro hac vice*)
ebinder@scott-scott.com
230 Park Ave., 17th Floor
New York, NY 10169
Tel.: (212) 223-6444
Fax: (212) 223-6334

Attorneys for Plaintiffs and the Proposed Class

ATTESTATION

Pursuant to Civil Local Rule 5-1(h)(3), I hereby attest that all signatories listed, and on whose behalf the filing is submitted, concur in the filing's content and have authorized the filing.

Dated: August 24, 2023

/s/Jeffrey A. Koncius

Jeffrey A. Koncius